日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 １月２５日

出願番号
Application Number: 特願２００１－０１７５１７

出願人
Applicant(s): 村田機械株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ８月２４日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号 出証特２００１－３０７４００７

#2

PATENT
81800.0180
Express Mail Label No. EL 713 632 478 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Art Unit: Not assigned
Yoshifumi TANIMOTO	Examiner: Not assigned
Serial No: Not assigned	
Filed: January 23, 2002	
For: METHOD OF TRANSMITTING EMAIL, DEVICE FOR IMPLEMENTING SAME METHOD, AND STORING MEDIUM STORING PROGRAM FOR TRANSMITTING EMAIL	

TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2001-017517 which was filed January 25, 2001, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: January 23, 2002

By: Lawrence J. McClure
Registration No. 44,228
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

【書類名】　特許願
【整理番号】　21790
【提出日】　平成13年 1月25日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 13/00
G06F 19/00
【発明の名称】　電子メール送信方法及び電子メール送信装置
【請求項の数】　5
【発明者】
【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内
【氏名】　谷本　好史
【特許出願人】
【識別番号】　000006297
【氏名又は名称】　村田機械株式会社
【代表者】　村田　純一
【代理人】
【識別番号】　100078868
【弁理士】
【氏名又は名称】　河野　登夫
【電話番号】　06(6944)4141
【選任した復代理人】
【識別番号】　100114557
【弁理士】
【氏名又は名称】　河野　英仁
【電話番号】　06(6944)4141
【手数料の表示】
【予納台帳番号】　001889
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9805283

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子メール送信方法及び電子メール送信装置

【特許請求の範囲】

【請求項１】　一のデータを複数の宛先へ電子メールにて送信する電子メール送信方法において、セッションキーを用いて前記データを暗号化するステップと、各宛先毎に定められた共通鍵夫々を用いて前記セッションキーを暗号化するステップと、前記暗号化したデータ及び前記暗号化したセッションキーを含む電子メールを送信するステップとを含むことを特徴とする電子メール送信方法。

【請求項２】　前記電子メールを送信するステップは、前記暗号化したデータ、前記暗号化したセッションキー及び前記複数の宛先を示したヘッダ情報を含む電子メールを送信することを特徴とする請求項１に記載の電子メール送信方法。

【請求項３】　前記電子メールを送信するステップは、前記暗号化したデータ及び一の前記暗号化したセッションキーを含む電子メールを、該セッションキーの暗号化に用いられた共通鍵に係る宛先に対して送信することを特徴とする請求項１に記載の電子メール送信方法。

【請求項４】　前記電子メールを送信するステップは、前記暗号化したデータ及びすべての前記暗号化したセッションキーを含む電子メールを、前記複数の宛先夫々に対して送信することを特徴とする請求項１に記載の電子メール送信方法。

【請求項５】　一のデータを複数の宛先へ電子メールにて送信する電子メール送信装置において、セッションキーを用いて前記データを暗号化する手段と、各宛先毎に定められた共通鍵夫々を用いて前記セッションキーを暗号化する手段と、前記暗号化したデータ及び前記暗号化したセッションキーを含む電子メールを送信する手段とを備えることを特徴とする電子メール送信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、暗号化されたデータを含む電子メールを同報送信する電子メール送

信方法及びその方法を実施するための電子メール送信装置に関する。

【０００２】

【従来の技術】

近年、コンピュータネットワークの急速な進展に伴い、安全なデータ通信を実現すべく、種々の暗号技術が注目されている。従来から、暗号化鍵及び復号鍵の両者の鍵が等しい暗号系である共通鍵暗号系、及び両者の鍵が異なる暗号系である公開鍵暗号系が広く利用されている。共通鍵暗号系の典型例としては米国商務省標準局が採用したＤＥＳ（Data Encryption Standards ）を、また公開鍵暗号系の典型例としてはＲＳＡ（Rivest Shamir Adleman ）を夫々挙げることができる。

【０００３】

一方、各ユーザの住所，氏名，電子メールアドレス等の個人を特定するＩＤ（Identity）情報を利用する暗号系が提案されている。この暗号系では、ＩＤ情報に基づいて送受信者間で共通の暗号化鍵を生成する。

【０００４】

このようなＩＤ情報に基づく暗号系であって、暗号文通信に先立って送受信者間での予備通信を必要としないものとして、ＩＤ－ＮＩＫＳ（ID-based non-interactive key sharing scheme ）が研究され提案されている。このＩＤ－ＮＩＫＳは、送受信者間で公開鍵，秘密鍵を交換する必要がなく、また鍵のリスト及び第三者によるサービスも不要であるので、任意のユーザ間で安全に通信を行うことができ、しかも、上述したように予備通信を必要としないので、ユーザの利便性が高いという利点を有している。そのため、将来の暗号系の中枢をなすものと期待されている。

【０００５】

図６はＩＤ－ＮＩＫＳのシステムの原理を示す説明図である。信頼できるセンタの存在を仮定し、このセンタを中心にして共有鍵生成システムを構成している。図６において、エンティティＡのＩＤ情報は、ハッシュ関数ｈ（・）を用いてｈ（ＩＤＡ）で表す。センタは、任意のエンティティＡに対して、センタ公開情報｛ＰＣｉ｝、センタ秘密情報｛ＳＣｉ｝及びエンティティＡのＩＤ情報ｈ（Ｉ

ＤＡ）に基づいて、以下の如く秘密鍵ＳＡｉを計算し、エンティティＡへ配布する。

ＳＡｉ＝Ｆｉ（｛ＳＣｉ｝，｛ＰＣｉ｝，ｈ（ＩＤＡ））

【０００６】

エンティティＡは、他の任意のエンティティＢとの間に行う通信の暗号化および復号のための共通鍵ＫＡＢを、エンティティＡ自身の秘密鍵｛ＳＡｉ｝、センタ公開情報｛ＰＣｉ｝及びエンティティＢのＩＤ情報ｈ（ＩＤＢ）を用いて以下の如く生成する。

ＫＡＢ＝ｆ（｛ＳＡｉ｝，｛ＰＣｉ｝，ｈ（ＩＤＢ））

また、エンティティＢも同様にエンティティＡとの間で用いる共有鍵ＫＢＡを生成する。ＫＡＢ＝ＫＢＡの関係が常に成立するのであれば、共有鍵ＫＡＢ，ＫＢＡをエンティティＡ，Ｂ間で暗号化鍵および復号鍵として利用することができる。

【０００７】

上述したＩＤ－ＮＩＫＳを利用して電子メールの送受信を行う場合について説明する。まず、電子メールの送信者及び受信者は、自己の電子メールアドレス（ＩＤ情報）に基づいて定められた秘密鍵を予めセンタから夫々取得しておく。そして、送信者は、受信者の電子メールアドレス（ＩＤ情報）に基づいて生成された公開鍵と前記取得した秘密鍵とに基づいて共通鍵を生成し、生成した共通鍵を用いてデータを暗号化し、その暗号化したデータを電子メールにて送信する。一方、受信者は、送信者の電子メールアドレス（ＩＤ情報）に基づいて生成された公開鍵と前記取得した秘密鍵とに基づいて共通鍵を生成し、受信した電子メール中のデータを前記生成した共通鍵を用いて復号する。

【０００８】

このようにして暗号化及び復号を行うことにより、安全な電子メールの送受信を容易に実現することができる。なお、このようなＩＤ－ＮＩＫＳにおける暗号通信には、例えば上述したＤＥＳ等を用いることができる。

【０００９】

【発明が解決しようとする課題】

ところで、同一のデータを電子メールにて複数の宛先に対して送信する場合、いわゆる同報送信を利用することができる。ここで同報送信とは、複数の宛先を指定した電子メールを一度送信するのみで、各宛先夫々に対して電子メールを送信することができる送信方法である。このような同報送信を利用する場合、各宛先夫々に対して電子メールを送信する場合に比し、少ない通信量で足りるという利点がある。

【００１０】

しかしながら、ＩＤ－ＮＩＫＳを利用する場合は、同一のデータを電子メールにて複数の宛先に送信するときであっても、上述したように各宛先の電子メールアドレス夫々を用いてデータの暗号化を行わなければならず、各宛先夫々に対して異なる電子メールを送信しなければならない。したがって、上述したような同報送信の利点を享受することができないという問題があった。

【００１１】

また、そのような利点を享受することができないばかりでなく、送信するデータに対する暗号化処理を宛先の数だけ実行しなければならないため、送信処理に相当な負荷がかかるという問題があった。

【００１２】

ところで、コンピュータネットワークにおけるデータ通信においては、従来から、送信するデータの保全を図るべく、そのデータを所定のセッションキーを用いて暗号化した後に送信する手法が採用されている。このようにしてセッションキーを用いることにより、改竄，なりすまし等の不正行為を未然に防止することが可能になる。

【００１３】

本発明はこのようなセッションキーの存在に鑑みてなされたものであり、セッションキーを用いて前記データを暗号化し、また各宛先毎に定められた共通鍵夫々を用いて前記セッションキーを暗号化した後、これら暗号化したデータ及びセッションキーを含む電子メールを送信することによって、送信するデータの暗号化処理は一度のみで足りるため、複数の宛先に対して暗号化されたデータを含む電子メールを送信する場合であっても従来に比しその送信処理の負荷を軽減する

ことができる電子メール送信方法及びその方法を実施するための電子メール送信装置を提供することを目的とする。

【００１４】

また本発明の他の目的は、暗号化したデータ及びセッションキーとともに、複数の宛先を示したヘッダ情報を含む電子メールを送信することによって、受信者側で同報送信された電子メールであることを容易に知ることができる電子メール送信方法を提供することにある。

【００１５】

【課題を解決するための手段】

第１発明に係る電子メール送信方法は、一のデータを複数の宛先へ電子メールにて送信する電子メール送信方法において、セッションキーを用いて前記データを暗号化するステップと、各宛先毎に定められた共通鍵夫々を用いて前記セッションキーを暗号化するステップと、前記暗号化したデータ及び前記暗号化したセッションキーを含む電子メールを送信するステップとを含むことを特徴とする。

【００１６】

第２発明に係る電子メール送信方法は、第１発明に係る電子メール送信方法において、前記電子メールを送信するステップは、前記暗号化したデータ、前記暗号化したセッションキー及び前記複数の宛先を示したヘッダ情報を含む電子メールを送信することを特徴とする。

【００１７】

第３発明に係る電子メール送信方法は、第１発明に係る電子メール送信方法において、前記電子メールを送信するステップは、前記暗号化したデータ及び一の前記暗号化したセッションキーを含む電子メールを、該セッションキーの暗号化に用いられた共通鍵に係る宛先に対して送信することを特徴とする。

【００１８】

第４発明に係る電子メール送信方法は、第１発明に係る電子メール送信方法において、前記電子メールを送信するステップは、前記暗号化したデータ及びすべての前記暗号化したセッションキーを含む電子メールを、前記複数の宛先夫々に対して送信することを特徴とする。

【００１９】

第５発明に係る電子メール送信装置は、一のデータを複数の宛先へ電子メールにて送信する電子メール送信装置において、セッションキーを用いて前記データを暗号化する手段と、各宛先毎に定められた共通鍵夫々を用いて前記セッションキーを暗号化する手段と、前記暗号化したデータ及び前記暗号化したセッションキーを含む電子メールを送信する手段とを備えることを特徴とする。

【００２０】

第１発明及び第５発明による場合、複数の宛先に対して送信すべきデータをセッションキーを用いて暗号化し、またそのセッションキーを前記宛先毎に定められた共通鍵を用いて暗号化する。そして、それら暗号化したデータ及び暗号化したセッションキーを含む電子メールを送信する。

【００２１】

これにより、複数の宛先に対して電子メールを送信する場合であっても、送信するデータの暗号化処理は一度のみで足りることになる。したがって、従来のように宛先の数だけ暗号化処理を行わなければならない場合に比し、暗号化処理に要する時間を短縮することができ、その結果電子メールの送信処理にかかる負荷を軽減することができる。

【００２２】

第２発明による場合、暗号化したデータ及び暗号化したセッションキーと共に、複数の宛先を示したヘッダ情報を含む電子メールを送信する。よって、受信者側で同報送信された電子メールであることを容易に知ることができる。

【００２３】

第３発明による場合、暗号化したデータと共に、暗号化したセッションキーのうち一のセッションキーを含む電子メールを、該一のセッションキーを暗号化する際に用いられた共通鍵に係る宛先に対して送信する。

【００２４】

このように、送信する電子メールに一の暗号化したセッションキーを含め、その暗号化に用いられた共通鍵に係る宛先に対してその電子メールを送信する場合、受信者は自己の共通鍵を用いて復号することができるセッションキー及びその

セッションキーを用いて復号することができるデータのみを受信することになる。よって、容易に復号して電子メールの内容を確認することができる。

【００２５】

第４発明による場合、暗号化したデータと共に、暗号化したセッションキーのすべてを含む電子メールを、すべての宛先夫々に対して送信する。

【００２６】

このように、同一の電子メールを複数の宛先に対して送信する場合、通常の同報送信の場合と同様に、その電子メールは一度のみ送信すれば足りる。したがって、各宛先夫々に対して電子メールを送信する場合に比し、少ない通信量で済む。

【００２７】

【発明の実施の形態】

以下、本発明をその実施の形態を示す図面に基づいて詳述する。なお、本発明では、後述するように、鍵共有方式としてＩＤ－ＮＩＫＳの枠組みを用いている。

（実施の形態１）

図１は、本発明の電子メール送信装置として機能するパーソナルコンピュータPC1,PC2,…,PCn（ｎは自然数）と、これらのパーソナルコンピュータPC1,PC2,…,PCnが接続されているコンピュータネットワークとの構成例を示すブロック図である。

【００２８】

図１において、NTW はコンピュータネットワークであるインターネットを示しており、このインターネットNTW には、インターネットNTW への接続業者である多数のプロバイダPR1,PR2,…,PRn（ｎは自然数）が接続されている。

【００２９】

プロバイダPR1,PR2,…,PRnは、これらと契約したクライアントに対して電子メールの送受信サービスを提供する電子メールサーバとして機能するサーバSV1,SV2,…,SVn（ｎは自然数）を夫々備えている。

【００３０】

またプロバイダPR1,PR2,…,PRnのサーバSV1,SV2,…,SVnには、ルータRT1,RT2,…,RTn（ｎは自然数）を介してクライアントとしてのパーソナルコンピュータPC1,PC2,…,PCnが接続されている。なお、ルータRT1,RT2,…,RTnに代えて、公衆電話回線の交換機を用いてもよい。

【００３１】

各パーソナルコンピュータPC1,PC2,…,PCnは、電子メールの送受信機能を有し、制御部１，モデム２，ＲＡＭ３，ハードディスク４，表示部５，及び操作部６等から構成される。

【００３２】

制御部１は、ＣＰＵ及びキャッシュメモリ等で構成されており、バス７を介して接続された各ハードウェア各部を制御すると共に、後述するハードディスク４に記憶されている種々のコンピュータプログラムを実行する。

【００３３】

モデム２は、インターネットNTW を介してデータ通信を行うための通信インタフェースであり、アナログ回線Ｌとの閉結及び解放の動作を行う。なお、モデム２の代わりに、ＤＳＵ（Digital Service Unit）を用いることにより、ベースバンド伝送方式のデジタル回線に接続するようにしてもよい。

【００３４】

ＲＡＭ３は、ＳＲＡＭ又はＤＲＡＭ等で構成され、制御部１において発生した一時的なデータを記憶する。

【００３５】

ハードディスク４は、読み書き可能な磁気ディスクから構成され、パーソナルコンピュータPC1,PC2,…,PCnの動作に必要な種々のコンピュータプログラムを予め記憶している。

【００３６】

また、このハードディスク４は、センタＣによって発行された秘密鍵を記憶している。図１に示すとおり、パーソナルコンピュータPC1 が備えるハードディスク４には、該パーソナルコンピュータPC1 を使用するユーザが所有する電子メールアドレスに基づいて生成された秘密鍵PRK1が記憶されているが、パーソナルコ

ンピュータPC2,…,PCnが備えるハードディスク４には、同様にして生成された秘密鍵PRK2 ,…,PRKn が夫々記憶されている。

【００３７】

なお、センタＣから秘密鍵PRK,PRK2 ,…,PRKn を取得する方法としては種々のものがあり、例えばインターネットNTW 等の通信ネットワークを介して取得してもよく、また秘密鍵PRK,PRK2 ,…,PRKn をフレキシブルディスクに記憶させ、そのフレキシブルディスクを郵送等により受け取ることによって取得するようにしてもよい。

【００３８】

表示部４は、ＣＲＴディスプレイ又は液晶表示装置（ＬＣＤ）等の表示装置であり、パーソナルコンピュータPC1,PC2,…,PCnの動作状態を表示したり、種々の入出力データの表示を行う。

【００３９】

操作部６は、パーソナルコンピュータPC1,PC2,…,PCnを操作するために必要なキーボード等の入力装置である。

【００４０】

次に、実施の形態１に係るパーソナルコンピュータPC1,PC2,…,PCnの動作について説明する。

図２は、実施の形態１に係るパーソナルコンピュータPC1 が電子メールを送信する場合の制御部１の処理手順を示すフローチャートである。なお、パーソナルコンピュータPC1 は、接続契約をしているプロバイダPR1 に対してユーザＩＤ，パスワード等を送出することによりログインしているものとする。また、ユーザは、複数の宛先に対して同一の内容の電子メールを送信しようとしているものとする。

【００４１】

まず、制御部１は、ユーザが操作部６を操作することによって入力された宛先の電子メールアドレス、及び電子メールとして送信する対象となるデータを受け付ける（Ｓ１０１，Ｓ１０２）。なお、上述したように、ユーザは複数の宛先に対して電子メールを送信しようとしているので、ステップＳ１０１では複数の電

子メールアドレスを受け付けることになる。

【００４２】

次に、操作部６を介して、ユーザから電子メールの送信指示命令を受け付けたか否かを判定する（Ｓ１０３）。ここで、送信をキャンセルする旨の命令を受け付けた場合、又は送信指示命令を所定時間内に受け付けなかった場合、送信指示命令を受け付けなかったと判定し（Ｓ１０３でＮＯ）、処理を終了させる。

【００４３】

一方、ステップＳ１０３にて送信指示命令を受け付けたと判定した場合（Ｓ１０３でＹＥＳ）、ステップＳ１０１にて受け付けた複数の電子メールアドレスを含むヘッダ情報を生成する（Ｓ１０４）。

【００４４】

次に、送信対象のデータを暗号化するためのセッションキーを生成する（Ｓ１０５）。なお、セッションキーは、このようにその都度新たなものを生成する以外にも、例えば所定数のものを予め用意しておき、それらを繰り返し使用するようにしてもよい。

【００４５】

次に、ステップＳ１０２にて受け付けた送信対象のデータを、ステップＳ１０５にて生成したセッションキーを用いて暗号化する（Ｓ１０６）。

【００４６】

そして、ステップＳ１０１にて受け付けた複数の電子メールアドレスのうち、一の電子メールアドレスを読み込み、その電子メールアドレスに基づいて生成された公開鍵とハードディスク４に記憶されている秘密鍵PRK1とを用いて共通鍵を生成する（Ｓ１０７）。

【００４７】

次に、このようにして生成した共通鍵を用いて、ステップＳ１０５にて生成したセッションキーを暗号化する（Ｓ１０８）。そして、前記読み込んだ電子メールアドレスを宛先に設定し、ステップＳ１０８にて暗号化したセッションキー及びステップＳ１０６にて暗号化したデータを用いて電子メールを作成する（Ｓ１０９）。

【００４８】

図３は、実施の形態１に係るパーソナルコンピュータPC1 の制御部１が作成する電子メールの構成例を示す概念図である。

図３に示すとおり、上述したステップＳ１０９にて作成した電子メールM1は、ヘッダ部HDR ，セッションキー部SK，及びデータ部DTにより構成される。

【００４９】

ヘッダ部HDR には、ステップＳ１０４にて作成したヘッダ情報が格納されている。このヘッダ情報には、上述したように宛先である複数の電子メールアドレスが含まれているので、受信者がこのヘッダ情報を参照することにより、受信した電子メールが同報送信されたものであることを容易に確認することができる。

【００５０】

またセッションキー部SKにはステップＳ１０８で暗号化されたセッションキーが、データ部DTにはステップＳ１０６で暗号化されたデータが夫々格納されている。

【００５１】

制御部１は、上述したような構成の電子メールM1をステップＳ１０９にて作成した後、その作成した電子メールM1を送信する（Ｓ１１０）。次に、ステップＳ１０１にて受け付けた複数の電子メールアドレスの全てに対して電子メールM1を送信したか否か、すなわち全ての宛先に電子メールM1を送信したか否かを判定する（Ｓ１１１）。ここで、まだ電子メールM1が送信されていない宛先があると判定した場合（Ｓ１１１でＮＯ）、全ての宛先に対して電子メールM1が送信されるまで、ステップＳ１０７乃至Ｓ１１０を繰り返す。その結果、全ての宛先に対して電子メールM1を送信したと判定した場合（Ｓ１１１でＹＥＳ）、処理を終了させる。

【００５２】

以上のようにしてパーソナルコンピュータPC1 から送信された電子メールM1は、サーバSV1 並びにサーバSV2,…,SVn等を介して、パーソナルコンピュータPC2,…,PCnによって受信される。電子メールM1を受信したパーソナルコンピュータPC2,…,PCnは、送信元の電子メールアドレスに基づいて生成された公開鍵及びハー

ドディスク４に格納されている秘密鍵PRK2 ,…,PRKn を用いて共通鍵を夫々生成し、生成した共通鍵を用いて受信した電子メールM1のセッションキー部SKに格納されている暗号化されたセッションキーを復号する。そして、その復号されたセッションキーを用いて、データ部DTに格納されているデータを復号する。これにより、各ユーザは電子メールM1の内容を確認することができる。

【００５３】

このように、セッションキーを用いることにより、複数の宛先に対して電子メールM1を送信する場合であっても、送信対象のデータの暗号化処理は一回のみ実行すれば済む。したがって、宛先の数だけ暗号化処理を行う必要がある場合に比し、暗号化処理に要する時間を短縮することができ、その結果電子メールM1の送信処理にかかる負荷を軽減することができる。

【００５４】

また、鍵共有方式としてＩＤ－ＮＩＫＳの枠組みを利用することにより、安全な電子メールの送受信を容易に実現することができる。

【００５５】

（実施の形態２）

上述したように、実施の形態１におけるパーソナルコンピュータPC1,PC2,…,PCnは、電子メールの宛先である複数の電子メールアドレスに対して暗号化されたデータを含む電子メールを夫々送信するため、電子メールの送信処理は複数実行する必要がある。これに対して、実施の形態２におけるパーソナルコンピュータPC1,PC2,…,PCnの場合は、後述するように、電子メールの送信処理が一回のみで足りる。

【００５６】

なお、実施の形態２におけるパーソナルコンピュータPC1,PC2,…,PCnの構成、及びこれらのパーソナルコンピュータPC1,PC2,…,PCnとコンピュータネットワークとの構成例については実施の形態１の場合と同様であるので図示及び説明を省略する。

【００５７】

以下、実施の形態２に係るパーソナルコンピュータPC1 の動作について説明す

る。

図４は、実施の形態２に係るパーソナルコンピュータPC1 が電子メールを送信する場合の制御部の処理手順を示すフローチャートである。なお、実施の形態１の場合と同様に、パーソナルコンピュータPC1 はプロバイダPR1 にログインしているものとし、ユーザは複数の宛先に対して同一の内容の電子メールを送信しようとしているものとする。

【００５８】

まず、制御部１は、ユーザが操作部６を操作することによって入力された宛先の電子メールアドレス、及び電子メールとして送信する対象となるデータを受け付ける（Ｓ２０１，Ｓ２０２）。

【００５９】

次に、操作部６を介して、ユーザから電子メールの送信指示命令を受け付けたか否かを判定する（Ｓ２０３）。ここで、送信をキャンセルする旨の命令を受け付けた場合、又は送信指示命令を所定時間内に受け付けなかった場合、送信指示命令を受け付けなかったと判定し（Ｓ２０３でＮＯ）、処理を終了させる。

【００６０】

一方、ステップＳ２０３にて送信指示命令を受け付けたと判定した場合（Ｓ２０３でＹＥＳ）、ステップＳ２０１にて受け付けた複数の電子メールアドレスを含むヘッダ情報を生成する（Ｓ２０４）。

【００６１】

次に、送信対象のデータを暗号化するためのセッションキーを生成する（Ｓ２０５）。なお、セッションキーは、このようにその都度新たなものを生成する以外にも、例えば所定数のものを予め用意しておき、それらを繰り返し使用するようにしてもよい。

【００６２】

次に、ステップＳ２０２にて受け付けた送信対象のデータを、ステップＳ２０５にて生成したセッションキーを用いて暗号化する（Ｓ２０６）。

【００６３】

そして、ステップＳ２０１にて受け付けた複数の電子メールアドレスのうち、

一の電子メールアドレスを読み込み、その電子メールアドレスに基づいて生成された公開鍵とハードディスク４に記憶されている秘密鍵PRK1とを用いて共通鍵を生成する（Ｓ２０７）。

【００６４】

次に、このようにして生成した共通鍵を用いて、ステップＳ２０５にて生成したセッションキーを暗号化する（Ｓ２０８）。次に、ステップＳ２０１にて受け付けた全ての宛先に係る電子メールアドレスを用いて前記共通鍵を生成したか否かを判定する（Ｓ２０９）。ここで、まだ共通鍵の生成に用いられていない電子メールアドレスがあると判定した場合（Ｓ２０９でＮＯ）、全ての宛先に係る電子メールアドレスが用いられるまで、ステップＳ２０７及びＳ２０８を繰り返す。

【００６５】

そして、全ての宛先に係る電子メールアドレスを用いて前記共通鍵を生成したと判定した場合（Ｓ２０９でＹＥＳ）、ステップＳ２０１に受け付けた全ての電子メールアドレスを宛先に設定し、ステップＳ２０８を繰り返すことにより生成された複数の暗号化されたセッションキー及びステップＳ２０６にて暗号化したデータを用いて電子メールを作成する（Ｓ２１０）。

【００６６】

図５は、実施の形態２に係るパーソナルコンピュータPC1 の制御部１が作成する電子メールの構成例を示す概念図である。

図５に示すとおり、上述したステップＳ２１０にて作成した電子メールM2は、実施の形態１における電子メールM1の場合と同様に、ヘッダ部HDR，セッションキー部SK，及びデータ部DTにより構成される。ただし、電子メールM1の場合はセッションキー部SKには一の宛先に係る暗号化されたセッションキーが格納されているのに対して、電子メールM2の場合は全ての宛先に係る暗号化されたセッションキーが格納されている。

【００６７】

制御部１は、上述したような構成の電子メールM2をステップＳ２１０にて作成した後、その作成した電子メールを送信し（Ｓ２１１）、処理を終了させる。

【００６８】

以上のようにしてパーソナルコンピュータPC1 から送信された電子メールM2は、サーバSV1 並びにサーバSV2,…,SVn等を介して、パーソナルコンピュータPC2,…,PCnによって受信される。電子メールM2を受信したパーソナルコンピュータPC2,…,PCnは、送信元の電子メールアドレスに基づいて生成された公開鍵及びハードディスク４に格納されている秘密鍵PRK2 ,…,PRKn を用いて共通鍵を夫々生成し、生成した共通鍵を用いて受信した電子メールM2のセッションキー部SKに格納されている複数の暗号化されたセッションキーの復号を試みる。その結果、復号することができたセッションキーを用いて、データ部DTに格納されているデータを復号する。これにより、各ユーザは電子メールM2の内容を確認することができる。

【００６９】

このように、全ての宛先に係る暗号化したセッションキーを含む電子メールM2を作成することにより、通常の同報送信の場合と同様に、サーバSV1に対して電子メールM2を一度送信するのみで、複数の宛先に対して電子メールが送信されることになる。したがって、各宛先夫々に対して電子メールを送信する場合に比し、少ない通信量で済む。

【００７０】

また、実施の形態１の場合と同様に、鍵共有方式としてＩＤ－ＮＩＫＳの枠組みを利用することにより、安全な電子メールの送受信を容易に実現することができる。

【００７１】

【発明の効果】

以上詳述した如く、請求項１に記載の電子メール送信方法及び請求項５に記載の電子メール送信装置によれば、セッションキーを用いて前記データを暗号化し、また各宛先毎に定められた共通鍵夫々を用いて前記セッションキーを暗号化した後、これら暗号化したデータ及びセッションキーを含む電子メールを送信することによって、送信するデータの暗号化処理は一度のみで足りるため、複数の宛先に対して暗号化されたデータを含む電子メールを送信する場合であっても従来

に比しその送信処理の負荷を軽減することができる。

【００７２】

また、請求項２に記載の電子メール送信方法によれば、暗号化したデータ及びセッションキーとともに、複数の宛先を示したヘッダ情報を含む電子メールを送信することによって、受信者側で同報送信された電子メールであることを容易に知ることができる。

【００７３】

また、請求項３に記載の電子メール送信方法によれば、暗号化したデータと共に、暗号化したセッションキーのうち一のセッションキーを含む電子メールを、該一のセッションキーを暗号化する際に用いられた共通鍵に係る宛先に対して送信することにより、受信者は自己の共通鍵を用いて復号することができるセッションキー及びそのセッションキーを用いて復号することができるデータのみを受信することになるため、容易に復号して電子メールの内容を確認することができる。

【００７４】

さらに、請求項４に記載の電子メール送信方法によれば、暗号化したデータと共に、暗号化したセッションキーのすべてを含む電子メールを、すべての宛先夫々に対して送信することにより、通常の同報送信の場合と同様に、その電子メールは一度のみ送信すれば足りるため、各宛先夫々に対して電子メールを送信する場合に比し、少ない通信量で済む等、本発明は優れた効果を奏する。

【図面の簡単な説明】

【図１】

本発明の電子メール送信装置として機能するパーソナルコンピュータと、これらのパーソナルコンピュータが接続されているコンピュータネットワークとの構成例を示すブロック図である。

【図２】

実施の形態１に係るパーソナルコンピュータが電子メールを送信する場合の制御部の処理手順を示すフローチャートである。

【図３】

実施の形態１に係るパーソナルコンピュータの制御部が作成する電子メールの構成例を示す概念図である。

【図４】

実施の形態２に係るパーソナルコンピュータが電子メールを送信する場合の制御部の処理手順を示すフローチャートである。

【図５】

実施の形態２に係るパーソナルコンピュータの制御部が作成する電子メールの構成例を示す概念図である。

【図６】

ＩＤ－ＮＩＫＳのシステムの原理を示す説明図である。

【符号の説明】

１　制御部

２　モデム

３　ＲＡＭ

４　ハードディスク

５　表示部

６　操作部

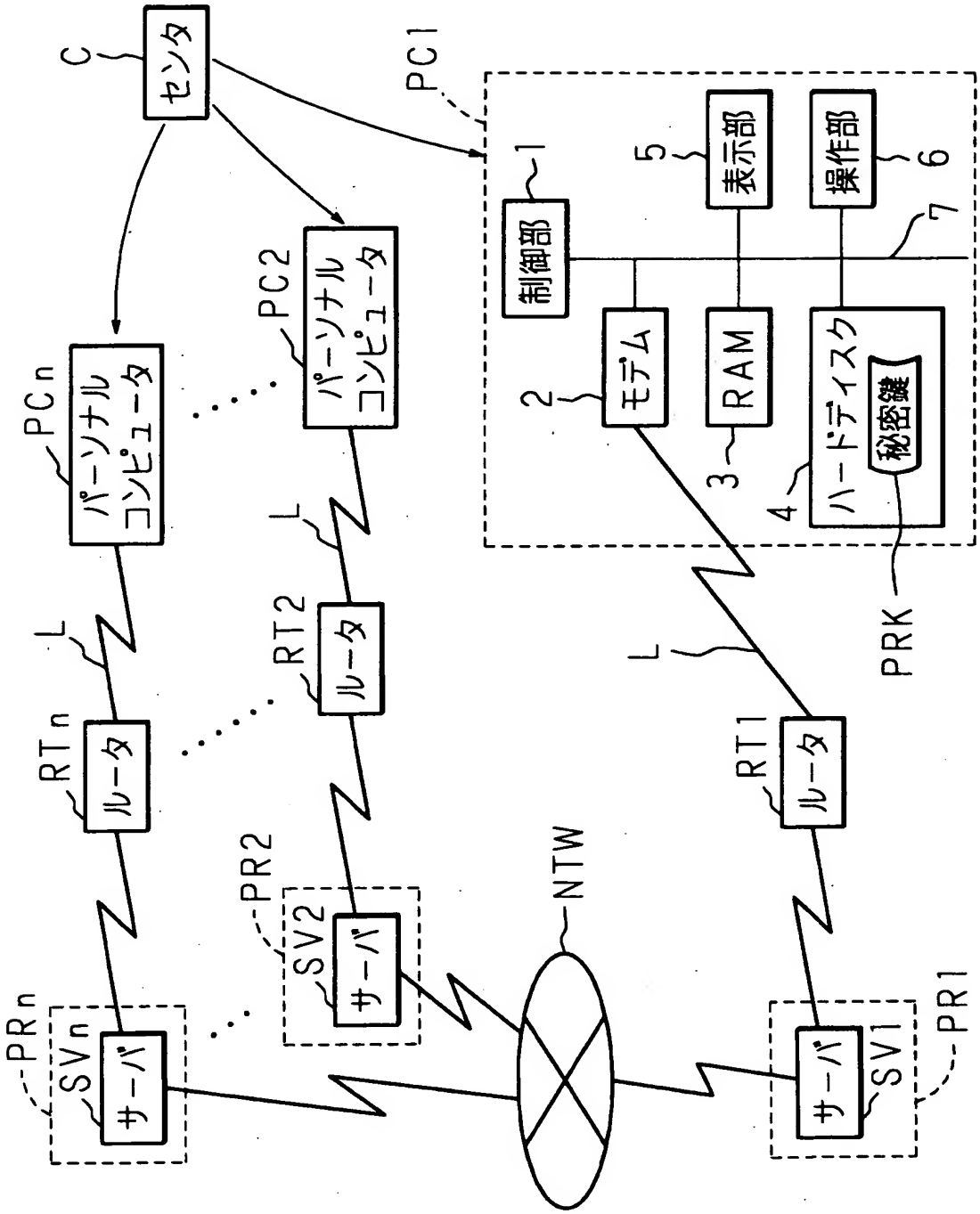
Ｃ　センタ

PC1 パーソナルコンピュータ

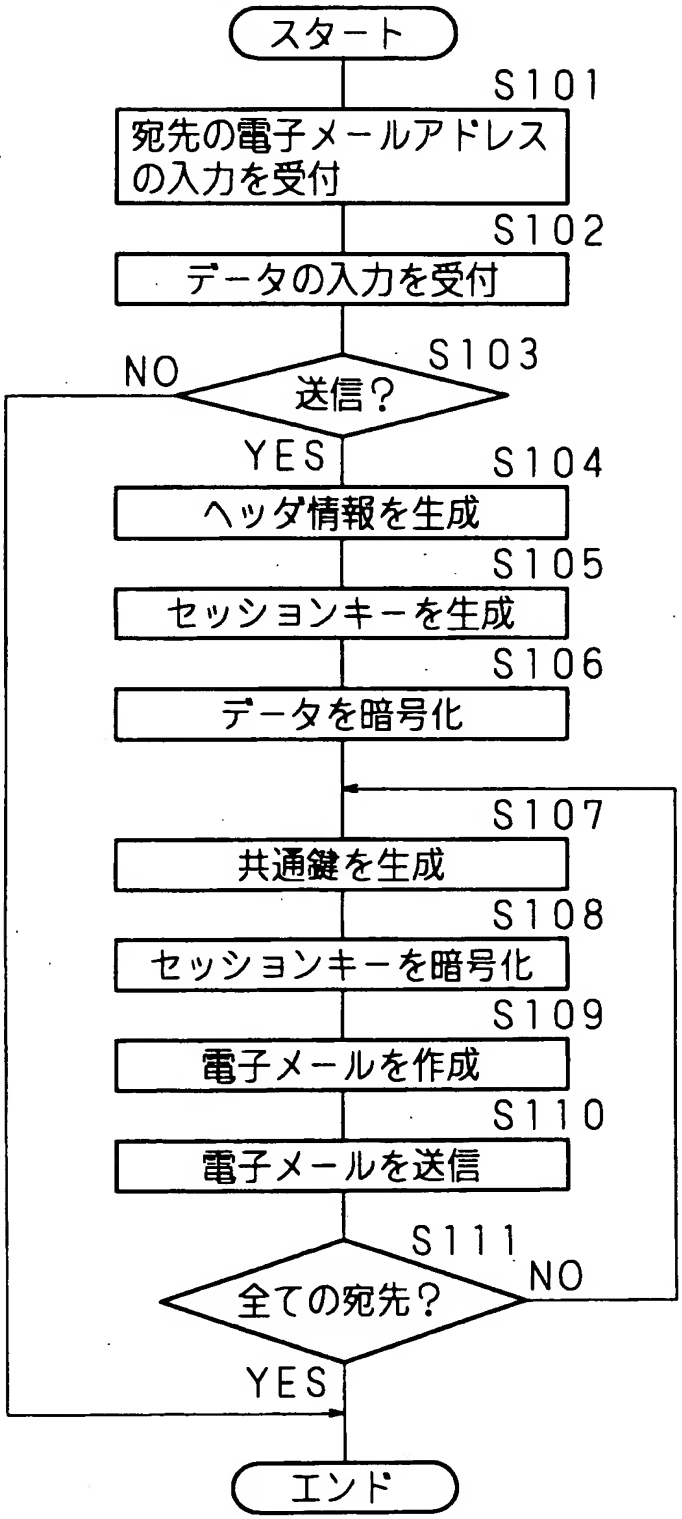
NTW　インターネット

【書類名】　　図面

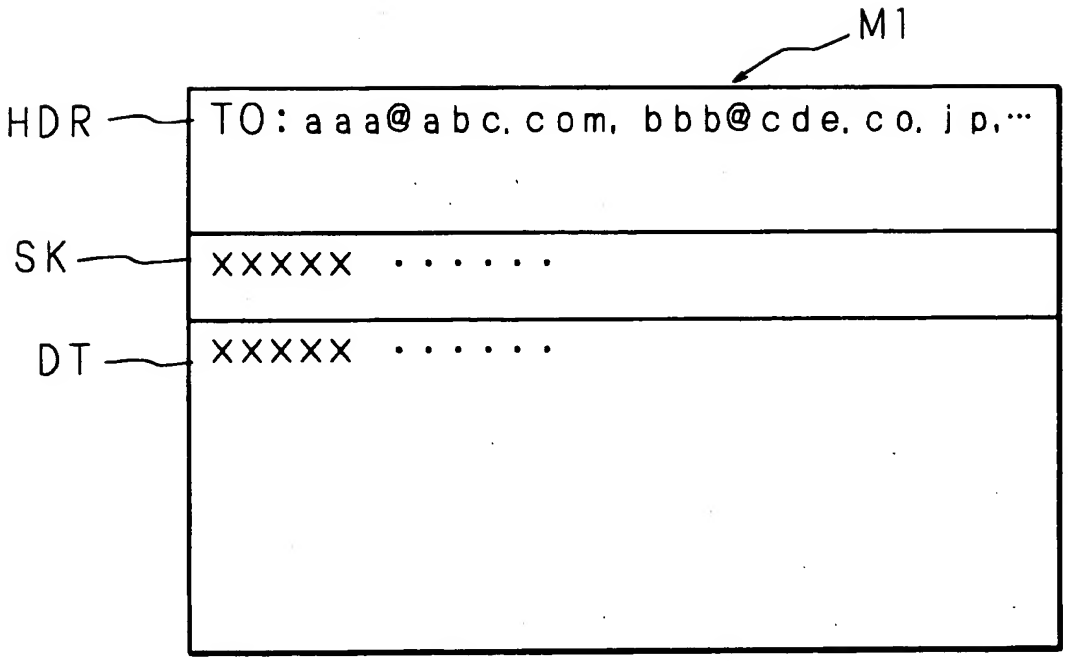
【図１】


C
センタ
PC1
制御部
1
モデム
2
RAM
3
ハードディスク
秘密鍵
4
表示部
5
操作部
6
7
PRK
PCn
パーソナル
コンピュータ
PC2
パーソナル
コンピュータ
L
RTn
ルータ
RT2
ルータ
RT1
ルータ
PRn
SVn
サーバ
PR2
SV2
サーバ
NTW
PR1
SV1
サーバ

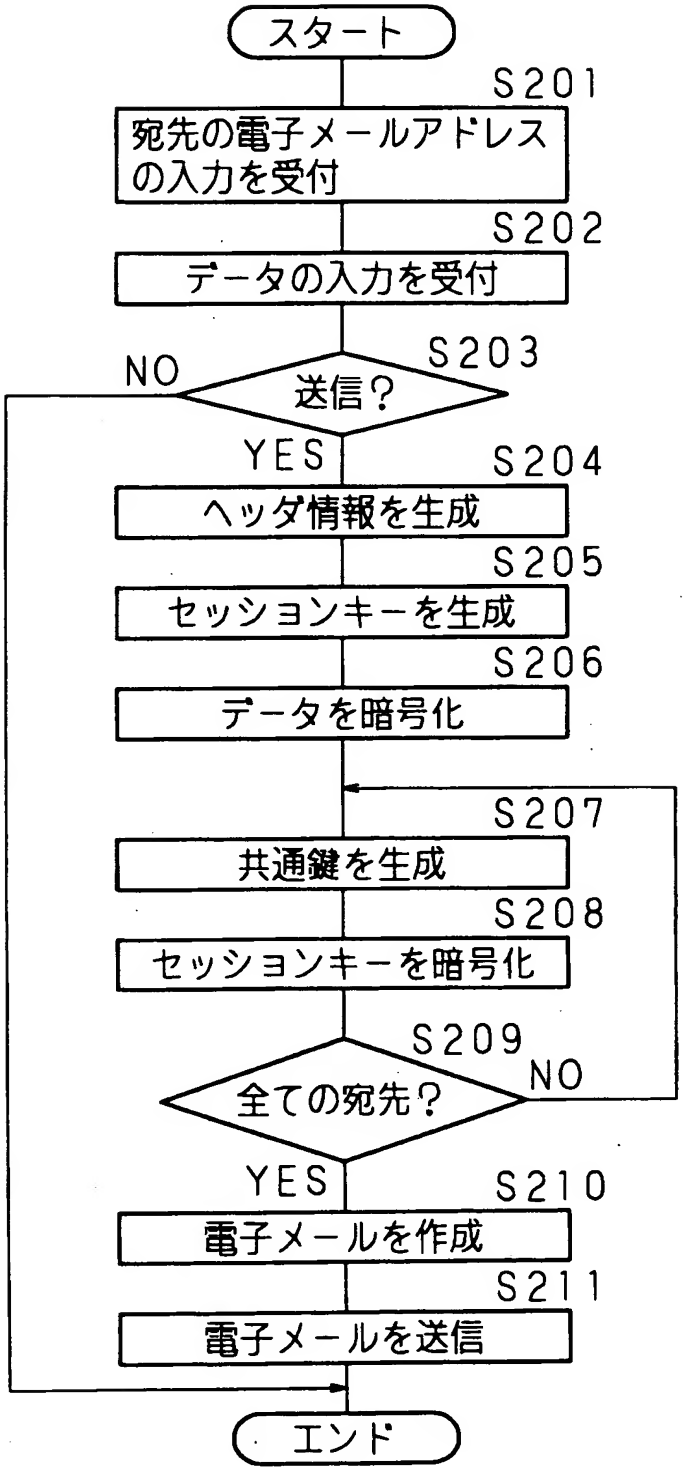
【図２】


スタート
S101
宛先の電子メールアドレスの入力を受付
S102
データの入力を受付
S103
送信？
NO
YES
S104
ヘッダ情報を生成
S105
セッションキーを生成
S106
データを暗号化
S107
共通鍵を生成
S108
セッションキーを暗号化
S109
電子メールを作成
S110
電子メールを送信
S111
全ての宛先？
NO
YES
エンド

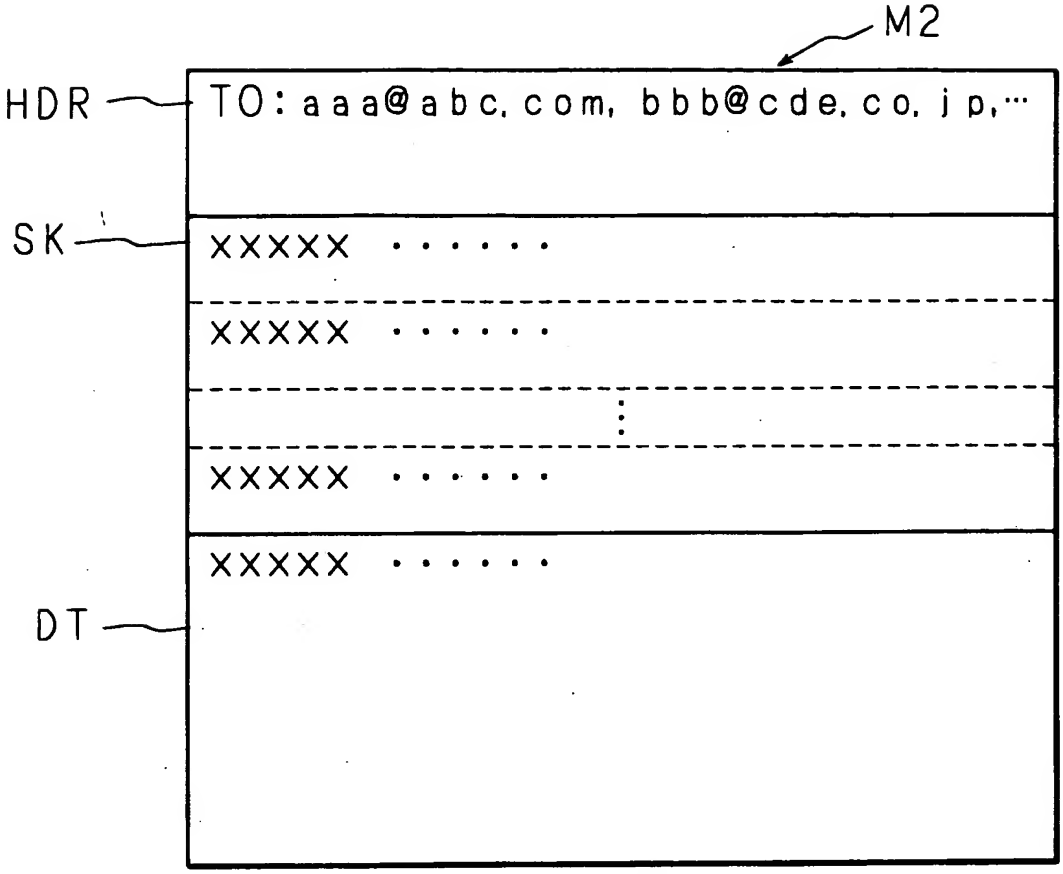
【図３】



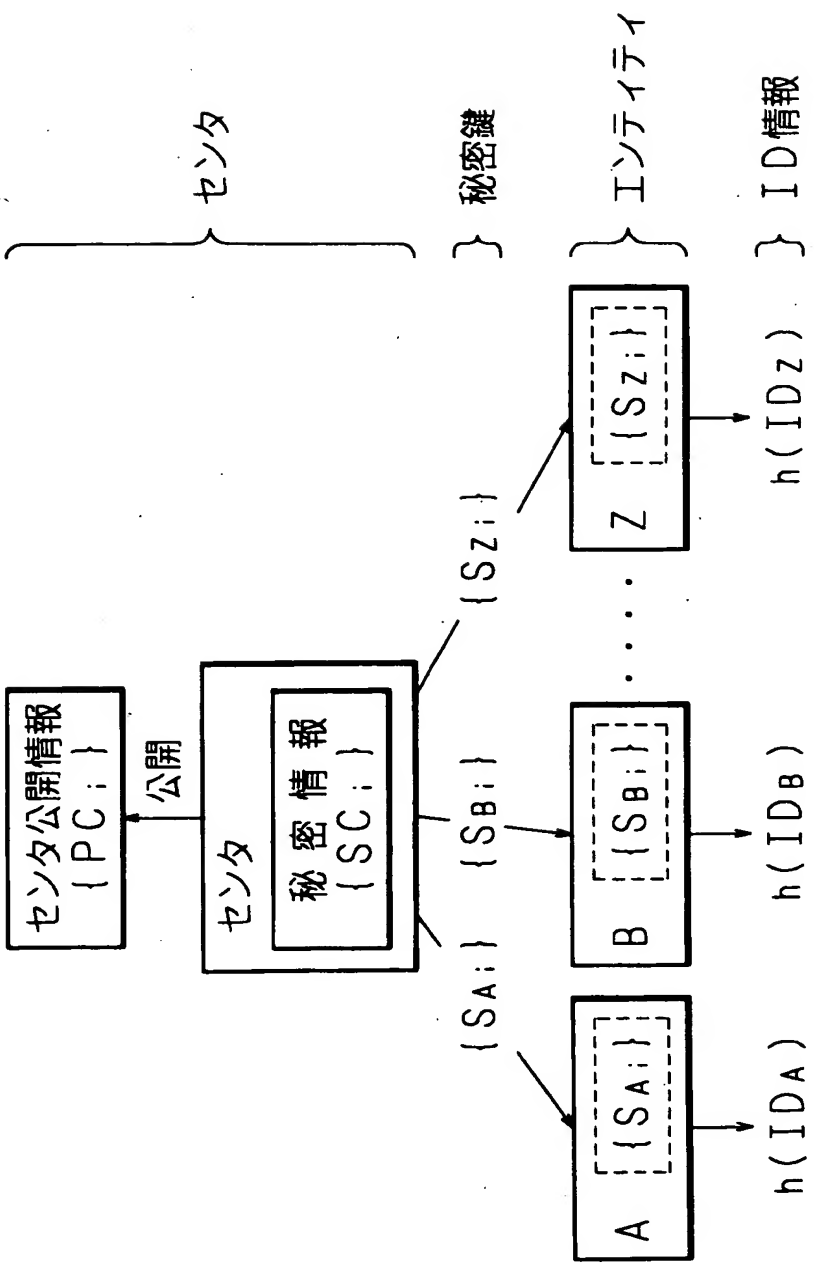
【図４】


スタート
S201
宛先の電子メールアドレスの入力を受付
S202
データの入力を受付
S203
送信？
NO
YES
S204
ヘッダ情報を生成
S205
セッションキーを生成
S206
データを暗号化
S207
共通鍵を生成
S208
セッションキーを暗号化
S209
全ての宛先？
NO
YES
S210
電子メールを作成
S211
電子メールを送信
エンド

【図５】


M2
HDR
TO：aaa@abc.com, bbb@cde.co.jp,…
SK
XXXXX ・・・・・・
XXXXX ・・・・・・
XXXXX ・・・・・・
XXXXX ・・・・・・
DT

【図６】


センタ
秘密鍵
エンティティ
ID情報
センタ公開情報
{PCi}
公開
センタ
秘密情報
{SCi}
{SAi}
{SBi}
{Szi}
A
{SAi}
B
{SBi}
Z
{Szi}
h(IDA)
h(IDB)
h(IDz)

【書類名】　　要約書

【要約】

【課題】　暗号化されたデータを含む電子メールを効率的に同報送信することができる電子メール送信方法及び電子メール送信装置の提供。

【解決手段】　パーソナルコンピュータPC1 は、同一のデータを複数の宛先に対して電子メールにて送信する旨の指示をユーザから受け付けた場合、セッションキーを生成し（Ｓ１０５）、生成したセッションキーを用いてデータを暗号化する（Ｓ１０６）。次に、各宛先の電子メールアドレスに基づいて生成された公開鍵及び予めセンタから取得した秘密鍵を用いて共通鍵を生成し（Ｓ１０７）、生成した共通鍵を用いてセッションキーを暗号化する（Ｓ１０８）。そして、前記暗号化したデータとセッションキーとを含む電子メールを各宛先夫々に対して送信する（Ｓ１１０）。

【選択図】　　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００６２９７〕

１．変更年月日　　１９９０年　８月　７日
［変更理由］　新規登録
住　所　京都府京都市南区吉祥院南落合町３番地
氏　名　村田機械株式会社